Amendments to the Claims

1   Claim 1 (currently amended): A computer program product for using biometrics on pervasive

2   devices for mobile identification, said computer program product embodied on a medium readable

3   by said pervasive device and comprising:

4   programmable code means for ~~capturing biometric data of a third party using~~ capturing,

5   using a biometric input reader which is attached to or incorporated within a mobile pervasive

6   device possessed by a first party, biometric data of a second party; and

7   programmable code means for identifying said [[third]] second party using said captured

8   biometric data by comparing said captured biometric data to previously-stored biometric data.

1   Claim 2 (original): The computer program product according to Claim 1, further comprising:

2   programmable code means for transmitting said captured biometric data from said mobile

3   pervasive device to a remote server;

4   programmable code means for retrieving, by said remote server, information from a

5   repository using said transmitted biometric data; and

6   programmable code means for returning said retrieved information to said mobile

7   pervasive device.

1   Claim 3 (original): The computer program product according to Claim 2, wherein said retrieved

2   information comprises a photograph of a party to whom said biometric data corresponds.

1   Claim 4 (original): The computer program product according to Claim 2, wherein said retrieved

Serial No. 09/537,068   -2-   Docket RSW9-2000-0002-US1

2   information comprises access rights of a party to whom said biometric data corresponds.

1   Claim 5 (currently amended): The computer program product according to Claim 2, further

2   comprising:

3   programmable code means for filtering, by said remote server, said retrieved information

4   based upon a determined identity of said [[third]] second party; and

5   wherein said returned retrieved information is said filtered retrieved information.

1   Claim 6 (original): The computer program product according to Claim 1, wherein said mobile

2   pervasive device further comprises a locally-stored repository containing said previously-stored

3   biometric data, and wherein said programmable code means for identifying compares, by said

4   mobile pervasive device, said captured biometric data to said previously-stored biometric data in

5   said locally-stored repository.

1   Claim 7 (original): The computer program product according to Claim 1, wherein said computer

2   program product is used to enable on-demand creation of a secure meeting site by repeating

3   operation of said programmable code means for capturing and said programmable code means for

4   identifying for each of a plurality of meeting attendees.

1   Claim 8 (currently amended): The computer program product according to Claim 1, wherein said

2   computer program product is used to exchange a trusted message by performing operation of said

3   programmable code means for capturing and said programmable code means for identifying

Serial No. 09/537,068   -3-   Docket RSW9-2000-0002-US1

4   wherein said [[third]] <u>second</u> party is a potential recipient of said trusted message.

1   Claim 9 (currently amended): A system for using biometrics on pervasive devices for mobile

2   identification, said system comprising:

3   a mobile pervasive device <u>possessed by a first party</u>;

4   a biometric input reader attached to or incorporated within said mobile pervasive device;

5   means for capturing biometric data of a [[third]] <u>second</u> party using said biometric input

6   reader; and

7   means for identifying said [[third]] <u>second</u> party using said captured biometric data by

8   comparing said captured biometric data to previously-stored biometric data.

1   Claim 10 (original): The system according to Claim 9, further comprising:

2   means for transmitting said captured biometric data from said mobile pervasive device to a

3   remote server;

4   means for retrieving, by said remote server, information from a repository using said

5   transmitted biometric data; and

6   means for returning said retrieved information to said mobile pervasive device.

1   Claim 11 (original): The system according to Claim 10, wherein said retrieved information

2   comprises a photograph of a party to whom said biometric data corresponds.

1   Claim 12 (original): The system according to Claim 10, wherein said retrieved information

Serial No. 09/537,068   -4-   Docket RSW9-2000-0002-US1

2   comprises access rights of a party to whom said biometric data corresponds.

1   Claim 13 (currently amended): The system according to Claim 10, further comprising:

2   means for filtering, by said remote server, said retrieved information based upon a

3   determined identity of said [[third]] second party; and

4   wherein said returned retrieved information is said filtered retrieved information.

1   Claim 14 (original): The system according to Claim 9, wherein said mobile pervasive device

2   further comprises a locally-stored repository containing said previously-stored biometric data, and

3   wherein said means for identifying compares, by said mobile pervasive device, said captured

4   biometric data to said previously-stored biometric data in said locally-stored repository.

1   Claim 15 (original): The system according to Claim 9, wherein said system is used to enable on-

2   demand creation of a secure meeting site by repeating operation of said means for capturing and

3   said means for identifying for each of a plurality of meeting attendees.

1   Claim 16 (currently amended): The system according to Claim 9, wherein said system is used to

2   exchange a trusted message by performing operation of said means for capturing and said means

3   for identifying wherein said [[third]] second party is a potential recipient of said trusted message.

1   Claim 17 (currently amended): A method for using biometrics on pervasive devices for mobile

2   identification, said method comprising the steps of:

Serial No. 09/537,068   -5-   Docket RSW9-2000-0002-US1

3   <u>capturing, using</u> ~~capturing biometric data of a third party using~~ a biometric input reader

4   attached to or incorporated within a mobile pervasive device <u>possessed by a first party, biometric</u>

5   <u>data of a second party;</u> and

6   identifying said [[third]] <u>second</u> party using said captured biometric data by comparing

7   said captured biometric data to previously-stored biometric data.

1   Claim 18 (original): The method according to Claim 17, further comprising the steps of:

2   transmitting said captured biometric data from said mobile pervasive device to a remote

3   server,

4   retrieving, by said remote server, information from a repository using said transmitted

5   biometric data; and

6   returning said retrieved information to said mobile pervasive device.

1   Claim 19 (original): The method according to Claim 18, wherein said retrieved information

2   comprises a photograph of a party to whom said biometric data corresponds.

1   Claim 20 (original): The method according to Claim 18, wherein said retrieved information

2   comprises access rights of a party to whom said biometric data corresponds.

1   Claim 21 (currently amended): The method according to Claim 18, further comprising the step

2   of:

3   filtering, by said remote server, said retrieved information based upon a determined

4   identity of said [[third]] second party; and

5   wherein said returned retrieved information is said filtered retrieved information.

1   Claim 22 (original): The method according to Claim 17, wherein said mobile pervasive device

2   further comprises a locally-stored repository containing said previously-stored biometric data, and

3   wherein said identifying step compares, by said mobile pervasive device, said captured biometric

4   data to said previously-stored biometric data in said locally-stored repository.

1   Claim 23 (original): The method according to Claim 17, wherein said method is used to enable

2   on-demand creation of a secure meeting site by repeating operation of said capturing step and said

3   identifying step for each of a plurality of meeting attendees.

1   Claim 24 (currently amended): The method according to Claim 17, wherein said method is used

2   to exchange a trusted message by performing operation of said capturing step and said identifying

3   step wherein said [[third]] second party is a potential recipient of said trusted message.

Serial No. 09/537,068   -7-   Docket RSW9-2000-0002-US1